

Notice of Allowability

Application No.

09/684,012

Examiner

Calvin L. Hewitt II

Applicant(s)

REZVANI ET AL.

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 11-21-05.
2. ☒ The allowed claim(s) is/are 1-17,19,20,22 and 23.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date 2-19-04, 9-21-05 *OK 12/10*
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Grant Pollock on 21 August 2005.

Status of Claims

2. The Application has been amended as follows-

In claim 1, in lines 9, 13, and 22, replace "token(s)" with "tokens".

In claim 1, line 19, replace "transmitting the data and the at least one tokens from the sender computer" with "transmitting the data and at least one of the N tokens from the sender computer".

In claim 1, line 21, replace "comparing the N token(s) transmitted from the sender computer" with "comparing the at least one of the N tokens transmitted from the sender computer".

In claim 1, line 23 replace "transmission(s)" with "transmissions".

Art.Unit: 3621

In claim 12, line 4, replace "similar checksum algorithm" with "equivalent checksum algorithm".

In claim 14, in lines 8, 11, and 18, replace "token(s)" with "tokens".

In claim 16, line 4, replace "a similar algorithm" with "an equivalent algorithm".

In claim 22, line 1, replace "the method set forth in claim 23, wherein the" with "the method set forth in claim 14, wherein the".

In claim 23, lines 9, 12, and 22, replace "token(s)" with "tokens"

In claim 23, line 19, replace "transmitting the data and the at least one tokens from the sender computer" with "transmitting the data and at least one of the N tokens from the sender computer".

In claim 23, line 21, replace "comparing the N token(s) transmitted from the sender computer" with "comparing the at least one of the N tokens transmitted from the sender computer".

3. Claims 1-17, 19, 20, 22, and 23 have been examined.
4. Claims 1-17, 19, 20, 22, and 23 have been allowed.

Reasons for Allowance

5. The present invention is directed to a method for authenticating data transferred between a sender and receiver. Message authentication is old and well-known. For example, digital signatures allow a message recipient to determine whether the message has been altered, while encryption ensures that only an intended recipient can access the message ("Applied Cryptography, Schneier, pages 28-33, 35, 38 and 39). The instant invention is directed to a method for authenticating messages by transmitting from a sender to a receiver N tokens, where N is a positive integer (i.e. N=1, 2, 3, ... etc.) and each token is a unique identifier. When the sender sends a message to the receiver, the sender transmits the message and at least one of the tokens therefore, when the receiver receives the message the receiver compares the received token or tokens to one or more transmissions for determining message authenticity. Unkenholz (US 4,429,180) discloses "one-time pads" for generating or selecting encryption keys where the pads are either transferred from one party to the next or are generated simultaneously by each party ('180, abstract; column 1, lines 10-38). Walker et al. (US 6,163,771) teach a system for issuing single-use credit card numbers and Cohen (US 6,422,462) teach single-use cards that are periodically distributed to a user ('462, column/line 3/55-4/11) and monitored for re-usage ('462, column/line 5/65-6/3). However, Applicant's method is distinguished from the prior art singly or in combination, as a user of a one-time pad would have no need for sending a key along with a message as both parties

already have the pad. Similarly, in Pickett (US 6,012,144), a user does not *resend* its token as the "Slice computer" already has it as is evidenced by the ability of the computer to present the token to the user ('144, figures 4 and 5; column 6, lines 22-45). Further, in order to read on the present invention, the card issuers of Walker et al. and Cohen, would have to send a block of cards to a user, then *resend* at least one of the block of cards, in order to allow the user to authenticate the card issuer. However, this teaches away from the clear teachings of Walker et al. and Cohen where the card numbers are used by the issuer to authenticate user transactions ('462, column/line 5/65-6/3; '771, figure 13).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- Walker et al. teach single-use credit card numbers
- Cohen teaches customizable credit card
- Unkenholz discloses one-time pads
- Watanabe et al. teach one-time pads

- "PC Dynamics Windows Security System 08/05/96", Newsbytes News Network, disclose tokens for authenticating the identity of a user

7. Any comments considered necessary by Applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

8. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Calvin Loyd Hewitt II whose telephone number is (571) 272-6709. The Examiner can normally be reached on Monday-Friday from 8:30 AM-5:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, James P. Trammell, can be reached at (571) 272-6712.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
c/o Technology Center 2100
Washington, D.C. 20231

or faxed to:

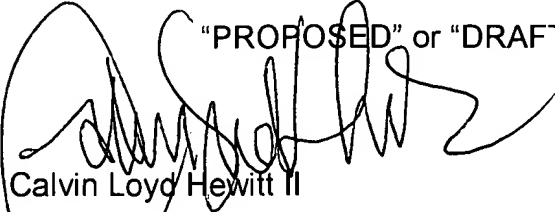
Art-Unit: 3621

(571) 273-8300 (for formal communications intended for entry and
after-final communications),

or:

(571) 273-6709 (for informal or draft communications, please label

"PROPOSED" or "DRAFT")



Calvin Loyd Hewitt II

November 21, 2005